Industry Canada Industrie Canada

PRINCIPLES FOR ELECTRONIC AUTHENTICATION

A Canadian Framework

May 2004

Canada

This publication is available in multiple formats upon request. Contact the Information Distribution Centre at the numbers listed below.

For additional copies of this publication, please contact:

Information Distribution Centre
Communications and Marketing Branch
Industry Canada
Room 268D, West Tower
235 Queen Street
Ottawa ON K1A 0H5

Tel.: (613) 947-7466
Fax: (613) 954-6436
E-mail: **publications@ic.gc.ca**

This publication, as well as additional background information on the Principles, is also available electronically on the World Wide Web at the following address: **http://strategis.ic.gc.ca/authen**.

Cat. No. Iu64-16/2004
ISBN 0-662-67949-0
54046B

CONTENTS

INTRODUCTION

All Canadians — individuals, businesses and governments — share an interest in ensuring that electronic communications are secure. As our use of public electronic networks continues to evolve, from searching the Internet for information to exchanging information and money online, we need greater assurance that these messages and transactions are secure and that our privacy is protected. Authentication of electronic communications can make a significant contribution to meeting this need and to building user confidence.

The Principles for Electronic Authentication are designed to function as benchmarks for the development, provision and use of authentication services in Canada. The Principles are intended to form the basis of codes of conduct, voluntary initiatives and guidelines tailored to the requirements of specific industries and government. For individual and business users of authentication services, the Principles are intended to be a useful source of information and benchmarks against which to evaluate services offered in the marketplace.

The Principles were developed by the Authentication Principles Working Group, convened by Industry Canada and with broad representation from industry, professional associations, consumer groups and various levels of government. The following organizations participated in the Working Group and supported the development of the Principles:

Bell Canada

Canadian Advanced Technology Alliance

Canadian Bankers Association

Canadian Bar Association

Canadian Institute of Chartered Accountants

Canadian Payments Association

Certified General Accountants Association of Canada

Deloitte & Touche LLP Canada

Digital Discretion Inc.

Gowling Lafleur Henderson LLP

Industry Canada (Electronic Commerce Branch and Office of Consumer Affairs)

Information Technology Association of Canada

Insurance Bureau of Canada

Juricert Services Inc.

Province of British Columbia

Province of Ontario

Public Interest Advocacy Centre

RBC Financial Group

Retail Council of Canada

Scotiabank

Spyrus Inc.

Standards Council of Canada

Teranet Inc.

Treasury Board of Canada Secretariat

University of Ottawa Law School

Visa Canada Association

WHY AND HOW TO USE THE PRINCIPLES

The Principles are intended to provide guidance for the development, implementation and use of authentication products and services in Canada. They complement the existing governance structure[1] for authentication by establishing benchmarks to ensure that authentication products and services embody sound business and market practices, meet the needs of Canadians and are accepted internationally.

The governance structure that applies to authentication services in Canada today consists of, among other instruments, the Government of Canada's 1998 Cryptography Policy, federal and provincial legislation, including the 2000 *Personal Information Protection and Electronic Documents Act*, the *Principles of Consumer Protection for Electronic Commerce*, developed in 2001, and the *Canadian Code of Practice for Consumer Protection in Electronic Commerce* (January 2004).

It is anticipated that the Principles for Electronic Authentication will be of greatest use to those involved in the design, development and deployment of authentication services and products. The Principles identify the functions and responsibilities of participants in authentication processes and provide a framework to assess and manage the risks that accompany these responsibilities. The Principles also identify security, privacy, disclosure and complaint-handling matters that need to be taken into account at each stage of the design, development, implementation and assessment of an authentication process.

Those involved with the design, implementation and ongoing operation of authentication processes are encouraged not only to respect the Principles but also to publicize them. The Principles should form the basis of codes of conduct, voluntary initiatives and guidelines that are tailored to the

1 The term *governance structure* refers to the range of policy tools, regulatory instruments and self-regulatory guidelines that relate to the development and implementation of authentication services in Canada.

requirements of specific industries and government. Such initiatives are strongly encouraged, and can provide strategic advantages in domestic and international markets.

The Principles are intended as a useful source of information and as benchmarks for individual and business users of authentication. While the Principles define the responsibilities of participants (Principle 1) and address aspects of risk management (Principle 2), they do not address the liabilities that could be borne by the various participants involved in authentication processes. In particular, the Principles do not address issues of consumer protection or liability, and should not be interpreted as allocating liability to end users of authentication services. Legislative or other measures may evolve to address the needs of end users, particularly the risk and liability assumed by consumers participating in authentication processes.

The authentication environment is dynamic and the technologies used will continue to evolve. Although every effort has been made to define principles that can encompass foreseeable developments, they are open to revision as needed to take into account significant technological advances, changes in market characteristics and international developments. Comments and views on the Principles are welcome at any time and should be addressed to:

Richard Simpson
Director General
Electronic Commerce Branch
Industry Canada
300 Slater Street, Room D2090
Ottawa ON K1A 0C8

Comments can also be provided by facsimile at (613) 941-0178 or by electronic mail at **authen@ic.gc.ca**.

The Principles will be reviewed at least every five years, or more frequently if necessary. The Authentication Principles Working Group is charged with the periodic review and revision of the Principles. The composition of this group will be assessed and adjusted as appropriate as the authentication environment evolves.

ABOUT THE PRINCIPLES

CONCEPTS AND TERMINOLOGY

The subject of the Principles is the authentication of electronic communications in its broadest sense. Therefore, the concepts and terms used in this document relate to all participants, actions and techniques comprising all aspects of authentication, whether considered from the technical, legal or business perspective. Each concept or term relates to the others; none should be considered in isolation.

Functions

For the purposes of the Principles, the authentication process is viewed as encompassing six functions. Their relative importance depends on the purpose and structure of the authentication process.

AUTHENTICATION ADMINISTRATION. Administering the measure or measures designed to confirm the attributes of a participant and those designed to support the credibility of a participant's claim to possess those attributes and thereby be authenticated.

SPECIFICATION. Establishing or selecting an authentication process and delivery mechanism.

END USE. Originating or receiving an authenticated electronic communication and relying on the authentication of the attributes.

STANDARDS DEVELOPMENT. Establishing standards that support the continued development of processes designed to facilitate authentication of electronic communications.

COMPLIANCE ASSESSMENT. Observing and making informed evaluations of the practices associated with authentication to ensure that appropriate policies, procedures and standards are being followed.

INFRASTRUCTURE PROVISION. Providing the capability that enables authentication, including functions to authenticate identity or the integrity of electronic communications.

Definitions

The Authentication Principles Working Group considered existing definitions, particularly those created by international standards groups such as the International Organization for Standardization (ISO), when developing the Principles. However, the broad scope of the Principles resulted in definitions that may not correspond to similar terms used by specific communities.[2]

AUTHENTICATION. A process that attests to the attributes of participants in an electronic communication or to the integrity of the communication.

ATTRIBUTES. Information concerning the identity, privileges or rights of a participant or other authenticated entity.

PARTICIPANT. An individual or organization participating in an authentication process, whether directly or through another authenticated entity, such as a data service or object, hardware device or software program.

ELECTRONIC COMMUNICATION. An electronic transmission, message or transaction.

INTEGRITY. Assurance that the information in an electronic communication has not been modified or corrupted during the process of communication.

Authentication is intended to promote trust in electronic communication. Participants in an electronic communication are provided with assurance that other participants have been authenticated using technological methods, and that those other participants, as well as the integrity of the communication itself, can be trusted to the degree specified by the authenticator (the designated authority that confirms the attributes of a participant or entity and then attests to them to other participants in the electronic communication).

2 For example, the definition of *authentication* encompasses "message authentication," which is commonly understood to refer to processes applied to ensure message integrity. Furthermore, a term that is not defined or used in connection with the Principles is *non-repudiation*. The term is commonly used to describe a technical standard to be met by an authentication process. However, the term is misleading in a more general context because it incorrectly implies a conclusion of law.

Participants rely on the authentication of an electronic communication to the extent that they can assess the reliability of the authentication. The technological methods and specifications used for authentication are often based on cryptographic techniques.

The act of authentication depends on some prior activity that authorizes participants, based on their presentation of certain specified attributes, to enter into an authenticated electronic communication. A participant's attributes may relate to a person's identity. As an alternative, the required attributes may identify the person's rights or privileges to enter into the electronic communication. In the latter case, a participant may not need to be identified personally to other participants.

Authentication processes frequently attest to the attributes of non-human entities. For example, an organization participating in an authentication process may choose to authenticate a server. In this case, the server's attributes may relate to the privileges it has been assigned to communicate with other servers or clients on the system.

Authorization is the responsibility of a designated authority. Many models are available for carrying out such authorization. For example, a simple exchange of information may require as authorization only the presentation of user identification and a password. An electronic system established to communicate highly confidential and private information may, by contrast, require in-person presentation of two or more pieces of reliable identification combined with unique personal characteristics, such as fingerprints. Yet another model designates an employer as the authority, who then authorizes a group of employees to engage in electronic communications on its behalf on the basis of individuals' job functions.

SCOPE AND NATURE OF THE PRINCIPLES

These Principles relate to the authentication of electronic communications in its broadest sense.

The Principles are intended to apply to authentication processes used in connection with electronic communications that take place between businesses or governments and other organizations, between organizations and individuals (consumers or citizens), and between individuals.

A range of relationships can exist between authenticators and end users, and among end users. Many of these relationships are governed by agreements. The Principles are intended to guide the development of these agreements and to apply to the full range of these relationships.

Parties to negotiated contracts are usually best able to determine which terms and conditions suit their particular needs. However, in situations in which a party may not have the opportunity to negotiate the terms of their interaction with the other party (or parties) to the transaction, the Principles are of particular importance.

The Principles should be considered and applied as a unified whole.

The provisions in the various Principles are interrelated and interdependent; they cannot achieve their purposes if they are implemented selectively, although not all Principles may apply in all cases. Those applying the Principles to define or implement authentication processes are encouraged to exceed the benchmarks that the Principles establish and to expand upon them to address the requirements of their particular security environment or application.

The Principles are expressed at a high level of generality and technological neutrality.

Canadians can choose from a variety of technologies to authenticate their electronic communications, according to the nature of the particular communication and the requirements of the participants.

The implementation of authentication processes also differs, depending on the business or legal objectives to be met, as well as the characteristics of the environment in which the electronic communication takes place, such as security and privacy needs and other legislative or regulatory obligations. These factors define the functionality required of an authentication process and, in some cases, even the type of authentication used.

The Principles are designed to foster a well-functioning, fair and competitive marketplace for authentication products and services.

Authentication processes should be effective, efficient, reliable and easy-to-use, and should respect the interests of individuals and organizations. Whenever possible, the Principles accommodate choice of technology, services and solutions, choice of the degree of reliance by end users, and choice of tools used to ensure compliance.

The Principles emphasize proportionality.

The degree of responsibility and risk that each participant in the authentication process assumes should be in proportion to the degree of knowledge and control that the participant can reasonably be expected to have and to exercise, as well as to the nature and value of the

electronic communication itself. Since participants can perform multiple functions in varying combinations, the degree of responsibility and risk assumed by any one participant may vary, depending on these functions.

The Principles emphasize data privacy.

The Principles recognize the existing and evolving legal framework for the protection of the privacy of personal information in Canada, and address how privacy protection standards apply to authentication. The Principles address the intersection of privacy-respecting and security-enhancing practices. The importance of privacy to Canadians requires those who design and implement authentication measures to consider how their systems can best respect privacy at every stage of the process.

The Principles have been developed to ensure compatibility with international developments in authentication.

Canada is committed to continued involvement in various international fora addressing the need for global frameworks for authentication. This participation ensures that Canada's approach is in step with that of other jurisdictions, enabling Canadian industry to be competitive in the international marketplace.

PRINCIPLES

PRINCIPLE 1: RESPONSIBILITIES OF PARTICIPANTS

Participants in an authentication process should be aware of the functions they are performing and of the responsibilities associated with those functions. Participants' responsibilities are proportional to the degree of knowledge and control they can reasonably be expected to have and to exercise.

All participants should act prudently and take reasonable steps to inform themselves of the nature of the authentication process, including its requirements and limitations, to protect information associated with the process, and to manage the risks to which they are exposed (see Principle 2).

Participants' specific responsibilities depend on the function or functions they carry out, as follows.

Authentication Administration

The administrator is responsible for following appropriate and trusted measures so that other participants may have confidence in the credibility of claimed attributes. When any part of the administration function is delegated to a third party, the administrator is responsible for ensuring that the third party also follows appropriate and trusted processes.

Specification

The specifying participant is responsible for choosing a system, such as an authentication infrastructure or process, that meets the privacy, security and other policy and legal requirements associated with an electronic communication. This may include the mechanism by which a participant's authority to enter into the electronic communication, and the integrity of the communication itself, can be ascertained.

End Use

The responsibility of end users to inform themselves about the authentication process is limited by the extent of clear and conspicuous information disclosed to them (see Principle 5). The responsibility of end users to protect information relating to the authentication process may be limited by legal or contractual obligations. Such obligations may

require disclosure of information concerning the process they use to determine the reliability of electronic communications.

Standards Development

Standards developers are responsible for ensuring that standards are robust, scalable and adaptive to encourage uniformity in authentication implementations. This responsibility extends to incorporating a wide range of views and best practices into proposed standards to ensure they are relevant, up-to-date and continuously applicable. Responsible standards development takes into account both existing and emerging technologies and international practices.

Compliance Assessment

Those who assess compliance are responsible for maintaining and applying a professional and up-to-date level of knowledge and practice so they can provide a reasoned and informed evaluation of authentication processes.

Infrastructure Provision

Infrastructure providers are responsible for following best practices and standards to implement and support the infrastructure that enables authentication.

PRINCIPLE 2: RISK MANAGEMENT

The risks associated with authentication processes for electronic communications should be identified, assessed and managed in a reasonable, fair and efficient manner.

The responsibilities of participants concerning risk management are proportional to the degree of knowledge and control that each participant can reasonably be expected to have and to exercise. It is recognized that the ability of participants to identify, assess and manage risk varies substantially, and that some types of participants (e.g. consumers and small enterprises) cannot reasonably be expected to identify, assess and manage risk to the same extent as participants that have access to more significant resources or who define the working relationships.

Identification

Risks should be identified to the extent possible. Risks may be financial — including immediate, direct and consequential damages arising from faulty execution or delay in execution of the communication — or may relate to, among other things, loss of confidentiality or privacy, damages to reputation, or identity theft.

Assessment

The seriousness and potential impact of risks should be assessed. When assessing risk, special attention should be paid to the circumstances under which the authentication process is relied upon. When evaluating and assessing risk, it can be helpful to take into account the responsibilities associated with each of the six functions (see Principle 1).

Management

Risks should be managed to the point of greatest economic efficiency by being assumed, avoided, re-allocated or mitigated. Risk is economically efficient when the residual risk that a participant bears after prudently managing risk does not outweigh the benefits gained from participating.

Role of Contracts

Contracts may be used to provide a framework for each participant's involvement. Contracts should be clear about the risks that each party is assuming and should allocate risk in a reasonable, fair and efficient manner. For contracts that are not freely negotiated among equal parties,[3] efforts may be needed to protect the interests of weaker parties.[4]

Decision Making

Regardless of the means used to allocate risk, the resulting allocation should be reasonable and fair and take into account the ability of participants to manage risk or absorb losses. It should also create incentives for those developing and implementing authentication processes to ensure that their products and services are secure and reliable.

3 An example of this is a contract that imposes terms of service on users.

4 Such efforts can be made at the industry sector level through the inclusion of provisions in codes, or at the government level through policy or legislation.

PRINCIPLE 3: SECURITY

All participants in an authentication process should be responsible and accountable for security, in proportion to their roles in that process. All participants have a responsibility to contribute to the mitigation of risk through sound security practices. However, infrastructure providers and those involved in authentication administration bear much of the burden to design and maintain systems based on policies and procedures that take into consideration legislation, regulation, policy, industry standards and the socio-cultural environment.[5]

The purpose of information security is to mitigate the risks inherent in the electronic sharing of information. Infrastructure providers and those involved in the specification and administration of authentication processes often take the initiative when designing and implementing security mechanisms, and therefore have an interest in raising awareness by informing other participants about these mechanisms and participants' role in their maintenance (for example, selecting and safeguarding user passwords). Security mechanisms should conform to generally accepted standards.

Protection, Detection and Response

As appropriate, all participants should be made aware and, at all times, be conscious of security risks, known threats and vulnerabilities, and available safeguards. In an authentication process, a security incident that affects a single participant may have implications for all participants. Participants should therefore act at all times to prevent such incidents, and should be ready and able to respond appropriately. Information about known threats, vulnerabilities and risks should be shared among participants, as appropriate, as an effective preventive measure, to enhance vigilance in

5 This principle accepts and adopts the Organisation for Economic Co-operation and Development's (OECD) *OECD Guidelines for the Security of Information Systems and Networks* (see page 24). The complete text of the Guidelines is available online at **www.oecd.org/dataoecd/16/22/15582260.pdf**.

detection and to ensure timely response. Effective information security measures should be proportional to the information risk and should respect the rights of participants, in keeping with the democratic principles of an open society.

Information technology evolves rapidly. It is therefore sound security management to ensure that all participants are reliably informed of new and existing threats, and of the role participants are expected to play in the prevention and detection of and response to security incidents.

Review and Assessment

The continual review and assessment of security programs is essential to ensure the ongoing efficacy of a security program. Those who establish authentication processes, and infrastructure providers in particular, in concert with the other participants in the authentication process, should verify and demonstrate their adherence to sound security management practices, each in proportion to the role they play. A person independent of the authentication process should conduct a periodic review of the security practices associated with the process. Such a review should be integral to accreditation and certification against generally accepted standards.

PRINCIPLE 4: PRIVACY

Organizations engaged in the design or operation of authentication processes should comply with the data protection standards set out in relevant codes of practice (privacy codes) in addition to complying with applicable legislation and jurisprudence (privacy laws).[6] In particular, the collection, use and disclosure of personal information[7] in the context of authentication should be minimized.

Identity-based authentication can conflict with privacy considerations. For example, stronger authentication may require the collection and comparison of more personal information. However, minimizing the collection, use and disclosure of personal information in the authentication context is fundamental for security as well as privacy reasons. Privacy safeguards can actually contribute to the security of authentication processes.

Authentication Administration

Authentication administration should involve the collection of personal information only when necessary. Any personal information collected should be used for no purpose other than authentication. Authentication of a business should focus on business attributes rather than personal attributes of individual employees.

---

6 General legislation governing data protection in the private sector that is currently in force includes the federal *Personal Information Protection and Electronic Documents Act* and privacy laws enacted in Alberta, British Columbia and Quebec. Other provinces and territories may choose to enact general data protection legislation. Federal, provincial and territorial privacy legislation that covers the public sector and sector-specific legislation protecting personal information may also apply.

The Canadian Standards Association's *Model Code for the Protection of Personal Information* (CAN/CSA-Q830-96) has been incorporated into the federal *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c.5, as Schedule 1 to that Act. The Code was developed by a multistakeholder working group and adopted by the Standards Council of Canada as a national standard in 1996. Many industry codes of practice also address data protection.

7 As defined in the *Personal Information Protection and Electronic Documents Act*: "any information about an identifiable individual."

If collection of personal information is required, such collection should be minimized. Any use or disclosure of personal information should also be minimized. Personal information should be collected, used or disclosed only with the informed consent of the individual.

Personal information should be retained only for the purpose of authentication.

Specification and Infrastructure Provision

Authentication processes should be designed to require that the least possible amount of personal information be collected, used and disclosed. Process design should take into account the access rights of participants and the obligation of organizations to make information available about their privacy policies. Organizations using authentication processes designed by others have a responsibility to ensure that those processes respect privacy.

End Use

End users of authentication processes and services should take reasonable measures to ensure that personal information within their control is protected from unauthorized collection, use or disclosure.

Standards Development

Authentication standards should be developed in full accordance with the privacy principles set out in privacy laws and codes. Privacy protection should explicitly be built into authentication standards. Standards developers should consider the coincidence of measures that contribute to protection of data privacy with those designed to ensure security of authentication processes.

Compliance Assessment

Compliance assessment should include assessment of whether and how the organization in question is complying with the privacy principles set out in privacy laws and codes. Compliance assessors should protect the confidentiality of personal information they deal with in the context of their assessments, in accordance with privacy laws and codes.

PRINCIPLE 5: DISCLOSURE REQUIREMENTS

Participants that offer authentication services should disclose information to the other participants to ensure that all participants are aware of the risks and the responsibilities associated with participation.

The information that is disclosed about authentication services should include policies, practices and procedures, as well as information about whether the services are periodically reviewed or audited. Appropriate disclosure requires the information to be provided in sufficient detail for the purpose, be in plain language and be conspicuous. All three factors will have a bearing on the knowledge other participants can reasonably be expected to have of the disclosed information.

Extent and Nature of Disclosure

Disclosure should *not* include security-related information that, if disclosed, would introduce vulnerabilities and increase risk. However, the amount and nature of information disclosed should be sufficient for participants to understand their responsibilities and to make informed risk-management decisions concerning reliance on the authentication. The extent and nature of the information may vary depending on whether the end user is an individual or an organization.

Notification

Participants should be notified of the availability of information and of any changes to the information. Evidence of receipt of notification may be required, depending on the nature of the authentication process and associated applications.

Relationship to Other Principles

Participants that offer authentication services should disclose their policy and practices concerning the collection of personal information. Principle 4 more fully addresses personal information and its disclosure. Disclosure requirements should also be considered in conjunction with Principle 1 (Responsibilities of Participants) and Principle 2 (Risk Management).

PRINCIPLE 6: COMPLAINTS HANDLING

Organizations implementing authentication processes should make available a complaints-handling process that enables participants to resolve complaints efficiently and effectively and to respond appropriately to non-compliance issues.

Complaints-handling processes should reflect the following.

Visibility

Information about how and where to direct complaints should be well publicized to all participants and their personnel and to other interested parties, and should include full information about the complaints-handling process.

Accessibility

The complaints-handling process should be easily accessible to all participants, and the organization should ensure that information is readily available on the details of resolving disputes. The process and supporting information should be easy for individuals with complaints to understand and use, be in plain language and be available in the languages in which the products and services were originally offered.

Responsiveness

Complaints should be dealt with promptly and thoroughly. Complaints should be assessed from a security perspective and resolved in priority, according to their potential negative impact on the participants involved or on the authentication implementation as a whole.

Fairness and Objectivity

Each complaint should be addressed in a balanced manner through the complaints-handling process, which should be fair to the complainant and the participant against whom the complaint is made.

Charges

Access to the complaints-handling process should be free-of-charge to the complainant.

Confidentiality and Privacy

Personal information concerning complainants should be available only where needed within the organization handling the complaint and must be actively protected from disclosure, unless the complainant expressly consents to its disclosure.

Accountability

Organizations should ensure that there is an identified individual or identifiable unit responsible for the systematic recording of complaints and outcomes, and for reporting on the actions and decisions of the organization with respect to complaints handling.

Continual Improvement

Continual improvement of the quality of authentication products and services is facilitated through the complaints-handling process, based on customer and other feedback. The complaints-handling process itself should be monitored on an ongoing basis, and reviewed and assessed in light of feedback.

Unresolved Complaints

When complaints cannot be resolved internally, organizations should be willing to use appropriate third-party dispute resolution processes upon request of the complainant, including those administered by private third parties. However, complainants should continue to have access to the justice system.

ADDITIONAL INFORMATION AND REFERENCES

ADDITIONAL INFORMATION

OECD Guidelines for the Security of Information Systems and Networks

1. Awareness

Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.

2. Responsibility

All participants are responsible for the security of information systems and networks.

3. Response

Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents.

4. Ethics

Participants should respect the legitimate interests of others.

5. Democracy

The security of information systems and networks should be compatible with essential values of a democratic society.

6. Risk Assessment

Participants should conduct risk assessments.

7. Security Design and Implementation

Participants should incorporate security as an essential element of information systems and networks

8. Security Management

Participants should adopt a comprehensive approach to security management.

9. Reassessment

Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.

REFERENCES

See **http://strategis.ic.gc.ca/authen** for a list of general references, as well as a list of domestic and international references and source documents specific to each Principle.